

Updated on 23/02/2024

**KPO Cooperative Society Group's External Labour Registry's
PRIVACY POLICY STATEMENT (as of 25/05/2018)**

General Data Protection Regulation (EU) 2016/679, Articles 12, 13, 14 and 19

1. Controller

KPO Cooperative Society

Phone: +358 20 780 7000

Postal address: P.O. Box 516, 67101 Kokkola

Street address: Prismantie 1, 67700 Kokkola

Business ID: 0242821-1

2. Contact details of data protection officer

tietosuojaavastaava@sok.fi

3. Officer in charge of register matters

tietosuoja.kpo@sok.fi

4. Name of the register

KPO Cooperative Society Group's External Labour Registry

5. Purpose of processing personal data

Processing of personal data of external labour. Personal data of external employees is processed to enable the identification of the individual and the performance of the task. Personal data is also processed for the purposes of statutory reporting on the activities of the controller and for other reporting purposes if necessary. Where necessary, personal data is also processed for the purpose of fulfilling other legal obligations.

6. Grounds for the processing of personal data

Legitimate interest – If the assignment agreement has been concluded with the employer or another contracting party (for example, temporary agency workers), the basis for processing personal data is mainly legitimate interest, with the exception of the name and telephone number of the emergency contact person and legal obligations. For Workplace, Office 365 cloud service and reporting that is not based on legal obligation, the basis for processing is mainly legitimate interest for all external workforce.

Consent – Name and telephone number of the emergency contact person. Consent of the data subject as regards the processing of location data

Legal obligation of the data controller – The controller may also need to process information on external employees in order to comply with legal obligations, for example to fulfil obligations arising from occupational safety legislation and to fulfil legal reporting obligations.

7. Description of the data controller's legitimate interest

Temporary agency workers: It is necessary for the controller to know who will perform a specific task for the company, as well as to process information necessary for the performance of the task. The data subject can reasonably expect that their personal data will be required for the activities of the controller in order to identify the person and perform the task.

Workplace: From the perspective of the controller's operations, it is justified and necessary to provide external workforce with a modern work communication channel that is independent of time and place. For the data subjects themselves, only the minimum data (contact details) will be exported to the services. In the case of Workplace, the data subject themselves has extensive opportunities to influence how actively and in what ways they participate in communications. Thus, the use of the service does not cause unreasonable inconvenience or risks to the data subject's privacy.

Office 365: Office 365 is a key tool and system for performing the task. Office 365 is a modern cloud service independent of time and place where the data subject has a wide range of possibilities to influence how they use Office 365 applications. For example, the data subject can manage the visibility of the documents they have created, and the files are visible only to the data subject by default.

Reporting not based on legal obligations:

It may be necessary for the controller to process external employee data for the purposes of reporting on the use of workforce and operational development. Reporting only includes purposeful information that is closely related to working in the company, and the processing is not surprising or unpredictable due to the significant relationship between the parties. It is highly unlikely that the processing would have a negative impact on the data subject.

8. Processed personal data and personal data groups

The controller processes only necessary personal data. The personal data collected will vary partly depending on the type of external workforce involved.

Temporary agency workers:

The name of the temporary worker is displayed in the shift roster of the shift planning system (Elli) or/and in the paper roster on the wall.

In addition, phone numbers of regular temporary workers may be displayed on the wall.

Temporary agency workers that have been assigned directly are mostly comparable with the workplace's employed workers. Their shift information is displayed in the shift planning system, they receive work clothes and can be added to the employee

self-service portal, through which they can see their shifts and express their wishes regarding shifts.

The person's name also appears in the seating order of the counters.

Access rights (electronic access badges) are signed off with a separate list.

Temporary agency workers are asked to sign a commitment to monitor age limits.

Information related to temporary agency workers is also exported to Massi (cash handling system).

Performance notes related to the collection of online shop products, such as which products a person has collected and when, are processed to assist in the management of supervision and contract obligations in S Group's Keräytin system.

Unpaid trainees:

A training agreement is concluded using the template of the educational institution or the TE Office, showing the name, contact information and personal identity code of the trainee.

Information about job familiarisation trainees (TET) is processed more narrowly according to the TET form in use, such as the person's name and grade.

Other temporary workforce:

The names are collected in a separate list, as well as how many hours each person has worked, based on which the agreed hourly rate is paid to the association (or other such) with which the use of workforce was agreed.

Transport company employees:

A person's name and phone number may be kept available.

9. Groups of data subjects

Temporary agency workers, unpaid trainees, other non-employed trainees, employees of subcontractors such as transport companies, and any other temporary workforce.

10. Data source and description of data sources if data is collected from public sources

The data in the register has been obtained mainly either from the temporary employment agency (or from its system, to which the controller has access), or from the data subject themselves, or from the party who sent them. Some of the information has been accumulated in the controller's systems or manual materials during the work.

11. Recipients of personal data

As a rule, personal data is not disclosed outside, unless there is a legal basis for disclosure. For example, the Occupational Safety and Health Act requires that the recipient of temporary agency work must, to the extent necessary, notify the

occupational healthcare services of the workplace and the occupational health and safety representative of the commencement of work.

However, an assessment of a person's performance may be handed over to an educational institution if their process requires it. For the purpose of tracking an order, the driver's name and phone number can be handed over to the online shop customer.

The personal data is processed in digital systems and services for the purposes specified in this privacy policy, such as Okta. We use external service partners in the provision of system and support services. Personal data can be transferred to said service providers insofar as the service providers participate in the implementation of measures within the framework of the relevant assignment.

We take care of the sufficient level of our partner's data protection according to what the law requires.

We disclose data to the authorities within the limits permitted and required by valid legislation when responding to authorities' requests for information.

12. Transfer of personal data to third countries or international organisations and data protection safeguards used

We use subcontractors to process personal data. Data is transferred outside the European Union (EU) or the European Economic Area (EEA) for the purpose of providing, maintaining and supporting the services to the extent necessary. We can perform these types of transfers if the European Commission has decided that the target country or organisation has a sufficient level of data protection or if we can otherwise ensure a sufficient level of protection of the personal data in accordance with applicable legislation, such as by using standard contractual clauses approved by the European Commission. You can read more about the standard contractual clauses approved by the European Commission [here Publications Office \(europa.eu\)](https://ec.europa.eu/euipo/publications-office)¹.

We require our subcontractors to agree to follow the data protection and information security requirements of legislation and us.

Personal data is transferred to outside the EU and the EEA when it is necessary for the technical implementation of the processing of personal data. In that case, the contractual partners are committed to ensuring that the protection mechanisms required by the General Data Protection Regulation are applied.

Our contract partners have signed service and data processing agreements compliant with the EU standard clauses that commit them to appropriate data protection arrangements.

Personal data is not transferred to any international organisations.

13. Period for storing personal data or criteria for determining the storage period

The personal data referred to in this privacy policy is only stored for as long as, and to the extent that, it is needed, and the data controller will utilise it for actions related to the reported purposes of processing.

Retention periods vary from process to process and are ultimately based on the controller's assessment of the need for each piece of information.

Traineeship agreements are retained until the traineeship has ended and the related measures have been completed (as standard, current year + one year).

Information related to the collection and delivery of online shop products is stored for a maximum of five years.

Shift lists are kept on paper for the current year + five years.

14. Rights of the data subject

The data subject has the right to access their own personal data as laid down in Article 15 of the General Data Protection Regulation (GDPR).

The data subject has the right to demand that the data controller corrects eventual incorrect or erroneous information as laid down in Article 16 of the Data Protection Regulation.

The data subject has the right to have their personal data removed in case the preconditions stated in Article 17 of the Data Protection Regulation are met.

The data subject has the right to restrict the processing of their personal data in case the preconditions stated in Article 18 of the Data Protection Regulation are met.

The data subject has the right according to Article 20 of the Data Protection Regulation to move the personal data from one system to another for the part for which the data was received from the data subject, its processing is automatic and its processing is based on consent or agreement.

The data subject has the right, based on Article 21 of the Data Protection Regulation, to object to the processing of the data that applies to them, in case the data was gathered in order to perform a task that concerns the common good, or based on legitimate interest, in case the other criteria included in the Article are met.

If a data subject wishes to exercise their rights or to obtain further information on the processing of their personal data, they may contact the controller named in this privacy policy.

Data subjects have the right lodge a complaint with the supervisory authority if they deem that the processing of their personal data violates the applicable data protection regulations.

15. Withdrawing consent

So far as the processing of the information is based on consent, the data subject has, according to Article 7 of the Data Protection Regulation, the right to withdraw their consent at any time. After the withdrawal, the data controller no longer has the right to use the personal data for such purposes that have no other grounds for processing except for the consent. Consent may be withdrawn by notifying it to the data controller.

16. Effects of not providing personal data on an agreement

The data controller cannot use an external worker who is not ready to provide the aforementioned personal data. The exception is data whose processing is based on the consent of the data subject. Consent may be withheld without penalty.

17. Significant information related to automated decision-making or profiling

No automated decision-making or profiling is associated with the personal data processing.

18. Impact of the processing of personal data and a general description of technical and organisational security measures

We diligently protect personal data throughout its lifecycle by employing the appropriate data protection and information security measures. System providers process personal data at secure server facilities. Access to personal data is restricted and our personnel is subject to a non-disclosure obligation.

At S Group, we protect personal data with, among other things, anticipatory risk management and security planning, data communication protection means, the continuous maintenance of information systems and backups, and by using secure hardware facilities, access control and security systems. After initial processing, the physical documents that contain personal data are kept in locked and fireproof storage areas. The granting and monitoring of user rights is a well-managed process. We regularly provide training for our personnel who participate in the processing of personal data, and ensure that our partners' personnel also understand the confidential nature of personal data and the importance of secure processing. We select our subcontractors with care. We continuously update our internal practices and guidelines.

If, despite all of our safeguards, personal data falls into the wrong hands, it is possible that the identity will be stolen or that the personal data will be otherwise misused. If we detect an event of this kind, we will start investigating it immediately and attempt to prevent any damage it may cause. We will inform the relevant authorities and data subjects of any information security breaches in accordance with legislative requirements.